METHOD AND APPARATUS FOR ENCODING AND STORING SESSION DATA

Abstract of the Disclosure

Session data is encoded in a tag-length-value format and encrypted using a modified encryption key. A session cookie is then formed by concatenating the length of the length of the secret, the length of the secret, the secret itself, and the encoded and encrypted configuration data. The session cookie is transmitted from a server computer to a client computer, where it is stored. Each time the client computer begins a new communications session with the server computer that generated the session cookie, the session cookie is transmitted from the client computer to the server computer. The server computer receives the session cookie from the client computer and extracts the secret stored in the session cookie. The server computer then creates the modified encryption key by inserting the secret into the standard encryption key at the predefined location. The server computer then utilizes the modified encryption key to decrypt the encoded session data stored in the session cookie. Once the encoded session data has been decrypted, the server computer decodes the tags contained in the encoded session data. For each tag, the server computer determines whether the tag is recognized as a valid tag. If the tag is a valid tag, the server computer utilizes the value associated with the tag to configure itself. If the tag is not a valid tag, the server computer ignores the tag and attempts to decode the next tag. The server computer continues decoding tags until no tags remain to be decoded. A new session cookie may be created and transmitted to the client computer. Periodically, the server computer may request the new session cookie from the client computer to determine if the communications session between the client computer and the server computer is still active. If no response or an invalid session cookie is received, the communications session between the client and server computers is terminated.